REMARKS

The Office Action dated October 11, 2007, and the Advisory Action dated January 22, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a supplemental response thereto.

Claims 1, 5, 12, 15, 19, 20 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claim 18 has been cancelled without prejudice or disclaimer. Claim 21 has been added. No new matter has been added. Claims 1-17, 19, and 20 are respectfully submitted for consideration.

Claims 1-4, 7-9, 10, and 15-20 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2004/0120328 to Adrangi et al. (Adrangi) in view of U.S. Patent Application Publication No. 2004/0120295 to Liu et al. (Liu). The Office Action took the position that Adrangi teaches some aspects of claims 1-4, 7-9, 10, and 15-20. The Office Action then cited Liu to cure the deficiencies of Adrangi. It is respectfully submitted that the subject matter is neither disclosed nor suggested in Adrangi and Liu.

Independent claim 1, upon which claims 2-14 are dependent, recites a system that includes a mobile node belonging to a home network located within a secure network, the mobile node having a network interface configured to communicate with other nodes, the mobile node having only one security association and only one mobility binding with a home agent so as to provide secure mobile connectivity that implements a mobile internet protocol home agent functionality. The system also includes a proxy home agent

connected to the home network and located within the secure network, wherein the proxy home agent is configured to provide a proxying functionality, the home agent located outside of the secure network, wherein the home agent is configured to provide a signaling and tunneling functionality and to notify the proxy home agent of the mobile node. The system further includes a virtual private network gateway located outside the secure network and configured to work in conjunction with the home agent. The system includes a demilitarized zone located outside the secure network, wherein the virtual private network gateway and the home agent reside in the demilitarized zone, and a first firewall between the secure network and the demilitarized zone. The system includes a second firewall between the demilitarized zone and an external network configured to deny communications from the external network with a source address in the known range.

Claim 15, upon which claims 16-18 are dependent, recites a method that includes establishing a proxy home agent located within the secure network to monitor data directed to the mobile node so as to secure communication between a mobile node associated with a home network in a secure network and a correspondent node. The method also includes establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node. The method further includes collecting data directed to the mobile node. The method additionally includes packaging the collected data in a virtual private network secure tunnel to an internal address of the

mobile node to create virtual protocol network packaged data. The method also includes tunneling the virtual protocol network packaged data to a current address of the mobile node. The method includes packaging the collected data in an internet-protocol-in-internet-protocol tunnel and sending it to a virtual protocol network device for virtual protocol network encryption and tunneling the virtual protocol network packaged data to the current address of the mobile node.

Claim 19 recites a system that includes means for establishing a proxy home agent located within a secure network to monitor data directed to a mobile node so as to secure mobile connectivity that implements mobile internet protocol home agent functionality via distributed components. The system also includes means for establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node. The system further includes means for collecting data directed to the mobile node and means for packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual private network packaged data.

The system additionally includes means for tunneling the virtual private network packaged data to a current address of the mobile node. The system also includes means for the home agent to communicate to the proxy home agent that the mobile node has moved outside its home network. The system additionally includes means for the home agent to communicate to the proxy home agent that the mobile node has come back to its

home network. The system also includes means for enabling the proxy home agent to create and remove a proxy address resolution protocol entry for a permanent address associated with the mobile node. The system includes means for providing a demilitarized zone located outside the secure network, wherein the virtual private network gateway and the home agent reside in the demilitarized zone, and a firewall between the secure network and the demilitarized zone. The system also includes providing means for providing a second firewall between the demilitarized zone and providing an external network configured to deny communications from the external network with a source address in the known range

Claim 20 recites a computer program embodied on a computer readable medium, the computer program being configured to control a processor to perform establishing a proxy home agent located within a secure network to monitor data directed to a mobile node. The computer program is also configured to control a processor to perform establishing a home agent configured to create only one security association with the mobile node and only one mobility binding with the mobile node and to notify the proxy home agent of the mobile node, and collecting data directed to the mobile node.

The computer program is further configured to control a processor to perform packaging the collected data in a virtual private network secure tunnel to an internal address of the mobile node to create virtual private network packaged data, and tunneling the virtual private network packaged data to a current address of the mobile node. The computer program is configured to control a processor to perform packaging the collected

data in an IP-in-IP tunnel and sending it to a virtual protocol network device for virtual protocol network encryption and tunneling the virtual protocol network packaged data to the current address of the mobile node.

As will be discussed below, Adrangi and Liu fail to disclose or suggest the elements of any of the presently pending claims.

Adrangi generally describes a seamless, secure roaming solution across enterprise firewalls. Specifically, a mobile node (MN) 140 may register with a home agent ("HA 130") when it exits its home subnet. During the registration process, the MN 140 informs HA 130 of MN 140's "care-of address" (hereafter "COA"), namely MN 140's address on its new subnet. See paragraphs [0012]-[0013]. HA 130 thereafter intercepts all IP packets addressed to MN 140 and reroutes the packets to MN 140's COA. As MN 140 moves from one subnet to another, MN 140 may obtain new COAs via Dynamic Host Configuration Protocol ("DHCP") or other similar protocols.

To ensure that HA 130 is able to properly route packets to MN 140, MN 140 must continuously update HA 130 with its new COA as it roams on Corporate Intranet 100. This configuration is commonly referred to as a "co-located" communications mode. Alternatively, Adrangi provides that when MN 140 leaves its home subnet, it may register with HA 130 via a foreign agent ("FA 135") on MN 140's new ("foreign") subnet. By registering with FA 135, MN 140 may use FA 135's IP address as its COA when registering with HA 130. In this scenario, HA 130 continues to intercept all packets addressed to MN 140, but these packets are now rerouted to FA 135, namely MN

140's COA as provided to HA 130. FA 135 examines all packets it receives, and sends the appropriate ones to MN 140 at its current location on the foreign subnet.

Applicants respectfully submit that the combination of Adrangi and Liu fails to disclose or suggest, at least, "a demilitarized zone located outside the secure network, wherein the virtual private network gateway and the home agent reside in the demilitarized zone; and a first firewall between the secure network and the demilitarized zone, and a second firewall between the demilitarized zone and an external network configured to deny communications from the external network with a source address in the known range," as recited in claim 1 and similarly recited in claim 19.

The Office Action took the position that Adrangi and Liu disclose all of the features of the above-discussed limitation. However, Applicants respectfully disagree. It is respectfully submitted that Adrangi fails to disclose or suggest, at least, "a second firewall between the demilitarized zone and an external network configured to deny communications from the external network with a source address in the known range," as recited in claims 1 and 19. Paragraph [0020], of Adrangi does not describe that the second firewall is located between the demilitarized zone and an external network. Further, the cited portion does not provide any information that the external network is configured to deny communications from the external network with a source address in the known range.

Therefore, the combination of Adrangi and Liu does not disclose or suggest all of the features of any of the presently pending claims. It is respectfully requested that the rejection be withdrawn.

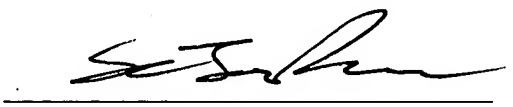
Furthermore, Applicants respectfully submit that the combination of Adrangi and Liu fails to disclose or suggest, in part, "packaging the collected data in an internet-protocol-in-internet-protocol tunnel and sending it to a virtual protocol network device for virtual protocol network encryption and tunneling the virtual protocol network packaged data to the current address of the mobile node," as recited in claim 15 and similarly recited in claim 20. Therefore, it is respectfully submitted that the combination of Adrangi and Liu does not disclose or suggest all of the features of any of the presently pending claims. It is respectfully requested that the rejection be withdrawn.

For the reasons explained above, it is respectfully submitted that each of claims 1-17 and 19-24 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-17 and 19-24 be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Sejoon Ahn
Registration No. 58,959

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

SA:dc

Enclosures: RCE
Check No. 18146